**USC UPSTATE**

**CSCI 455: Computer Security**

**Spring 2019**

**Homework Assignment 2**

**Problem 1**

1. Describe how an attacker can obtain the one-time pad that is used to encrypt a message, given both the message and the ciphertext, and explain why your method works.

Answer: Given both the original message and the ciphertext, an attacker can calculate the number each letter is shifted by comparing the two. I.e. A -> E would be a 4 letter shift. Doing this for the whole message, one can find the original one-time pad.

1. Suppose that two equal-sized messages *M*1 and *M*2 are encrypted with the *same* one-time pad and let *C*1 and *C*2 be the resulting ciphertexts. Suppose further that an attacker captures both ciphertexts *C*1 and *C*2, and knows one of the two messages, say *M*1. Based on Part a), describe how the attacker can obtain the other message *M*2, and explain why your method works.  
     
   Answer: If we have M1, C1 and C2, we can use the method of part a to find the one-time pad using M1, C1. Since both ciphertexts used the same one-time pad, one can just apply the pad to C2 to decrypt it and get the original message.
2. Let’s think about a more realistic situation than part b) that the attacker captures both ciphertexts *C*1 and *C*2, but does not know message *M*1. Based on part b), can you provide an example showing that the attacker can still obtain the message *M*2 ? You can do research online and find approaches. By answering this question, you can have an idea on how an attacker can do in practice and why the one-time pad cannot be used more than once.

Answer: Using a simple and common word, such as “the”, one can exclusive-or the word against the XOR of C1 and C2. If the common word appears in one of the plaintext, you will get the plaintext of the other cipher in that spot. Doing this you can narrow down the plain text enough to possibly make both readable.